

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.




# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,103	04/30/2001	Dmitry O. Gryaznov	002.0160.01	5029
22895	7590	09/10/2004	EXAMINER	
PATRICK J S INOUE P S 810 3RD AVENUE SUITE 258 SEATTLE, WA 98104			COLIN, CARL G	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 09/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/846,103	<b>Applicant(s)</b> GRYAZNOV ET AL. 	
	<b>Examiner</b> Carl Colin	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 30 April 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 April 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
     If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
         1. ☐ Certified copies of the priority documents have been received.  
         2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
     \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
     a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

### DETAILED ACTION

1. Pursuant to USC 131, claims 1-44 are presented for examination.

#### *Specification*

2. The disclosure is objected to because of the following informalities: on page 12, line 16, reference number "133" should be --142--. Appropriate correction is required. Applicant is requested to review the application to correct such errors.

- 2.1 The abstract of the disclosure is objected to because of the first sentence that repeats information given in the title and implies "the disclosure describes". Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

- 2.2 The disclosure is objected to because it contains embedded hyperlinks and/or other form of browser-executable codes (see p.2, line 2). Applicant is required to delete the embedded hyperlinks and/or other form of browser-executable codes. See MPEP § 608.01.

***Drawings***

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because the following reference number is not consistent with the drawings: on page 5, line 30, reference number 16 describes “a macro virus family” whereas on page 16, it refers to “a macro virus checker”. Applicant is required to carefully review the application to correct such errors.

A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

**Claims 4, 20, 35, and 40** and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1 Regarding **claims 4, 20, 35, and 40** the phrase "substantially common" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "substantially similar"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(b).

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5.1 **Claims 1-11, 14-27, 30-44** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 5,951,698 to **Chen et al.**

5.2 **As per claims 1, 17, 33, 34, 39, and 44, Chen et al.** discloses a method and system for identifying a macro virus family using a macro virus definitions database, comprising: maintaining a macro virus definitions database comprising a set of indices and macro virus definition data files with each index referencing one or more of the macro virus definition data files and each macro virus definition data file defining macro virus attributes for known macro viruses; organizing the sets of the indices and the macro virus definition data files according to

Art Unit: 2136

macro virus families in each respective index and macro virus definition data file set, for example (see column 14, line 52 through column 15); comparing a suspect string to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database, for example (see column 14, line 52 through column 15); and determining each macro virus family to which the suspect string belongs from the index for each macro virus definition data file at least partially containing the suspect string or file, for example (see column 13, line 20 through column 14 and column 14, line 52 through column 15).

**As per claims 2 and 18, Chen et al.** discloses the limitation of further comprising: the macro virus definition data files being indexed into the macro virus families categorized by a replication method employed, for example (see column 8).

**As per claims 3 and 19, Chen et al.** discloses the limitation of wherein the suspect string comprises part of a suspect file comprising a plurality of individual suspect strings, for example (see columns 14-15).

**As per claims 4 and 20, Chen et al.** discloses the limitation of further comprising: the macro virus checker identifying a replication method substantially common to a plurality of the individual suspect strings in the suspect file, for example (see column 14, lines 16 et seq.).

**As per claims 5 and 21, Chen et al.** discloses the limitation of further comprising: the macro virus checker identifying the macro virus family by which the common replication method is indexed, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

**As per claims 6 and 22, Chen et al.** discloses the limitation of further comprising: the macro virus definitions database storing string constants common to each macro virus family in the macro virus attributes for the macro virus definition data files, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15); and the macro virus checker comparing the suspect string to the string constants in the one or more macro virus definition data files for each macro virus family, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15).

**As per claims 7 and 23, Chen et al.** discloses the limitation of further comprising: a parameter specifying a threshold to matches of commonly shared string constants, for example (see column 15, lines 1-12).

**As per claims 8, 24, 38, and 43, Chen et al.** discloses the limitation of further comprising: a parameter specifying a minimum length of commonly shared string constants, for example (see column 15, lines 1-12).



**As per claims 9 and 25, Chen et al.** discloses the limitation of further comprising: the macro virus definitions database storing source code text common to each macro virus family in the macro virus attributes for the macro virus definition data files; and the macro virus checker comparing the suspect string to the source code text in the one or more macro virus definition data files for each macro virus family, for example (see column 14).

**As per claims 10, 26, 37, and 42, Chen et al.** discloses the limitation of further comprising: a parameter specifying a threshold to matches of commonly shared source code text, for example (see column 12, lines 3-40 and column 13, line 20 through column 14).

**As per claims 11 and 27, Chen et al.** discloses the limitation of further comprising: a set of keywords used in the stored source code text to identify each replication method employed, for example (see column 12, lines 3-40 and column 13, line 20 through column 14).

**As per claims 14 and 30, Chen et al.** discloses the limitation of further comprising: the macro virus checker parsing macro virus attributes from one or more file objects and analyzing the macro virus definition data files by index for each macro virus family, for example (see columns 12-14).

**As per claims 15 and 31, Chen et al.** discloses the limitation of further comprising: the macro virus checker cross referencing at least one of a string constant and source code text from

the parsed macro file attributes against the macro virus attributes defined in the virus definition data files, for example (see columns 12-14).

**As per claims 16 and 32, Chen et al.** discloses the limitation of further comprising: the macro virus checker iteratively retrieving each macro virus definition data file using the index for each macro virus family and providing the macro virus attributes defined in the retrieved macro virus definition data file, for example (see columns 12-14).

**As per claims 35 and 40, Chen et al.** discloses the limitation of further comprising: each macro virus family defined according to a replication method substantially common to each of the macro virus definition data files associated with one such index, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

**As per claims 36 and 41, Chen et al.** discloses the limitation of further comprising: the macro virus definitions database storing at least one of string constants and source code text common to each macro virus family in the macro virus attributes for the macro virus definition data files, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15 and column 12, lines 3-40 and column 13, line 20 through column 14); and the macro virus checker comparing the suspect string to the at least one of the string constants and the source code text in the one or more macro virus definition data files for each macro virus family, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15 and column 12, lines 3-40 and column 13, line 20 through column 14).

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6.1 **Claim 12-13 and 28-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,951,698 to **Chen et al.**

6.2 **As per claims 12, 13, 28, and 29, Chen et al.** substantially teaches discloses the limitation of updating information when new virus is found which includes updating the index by writing new information to corresponding set of data that meets the recitation of further comprising: the macro virus checker resetting the index referencing one or more of the macro virus definition data files for at least one macro virus family and creating a new macro virus definition data file entry comprising an index referencing one or more macro virus definition files, for example (see column 9, lines 15 see also figure 9) and discloses the new macro virus definition data file entry defining the macro virus attributes by storing at least one of a. string constant and source code text, for example (see column 9 through column 10, line 27), **Chen et**

al. is silent about resetting the index referencing one or more data files because it is obvious to one skilled in the art that to add new identifier the order may need resetting. Therefore, resetting the index referencing one or more of the macro virus definition data files for at least one macro virus family does not depart from the spirit and scope of the invention disclosed by **Chen et al.**

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the use virus identification using virus definition database. Many of the claimed features are disclosed in these references.

US Patents: 6,067,410, Nachenberg; 5,414,833, Hershey et al; 5,485,575, Chess et al


7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

*cc*

Carl Colin  
Patent Examiner  
September 3, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100